RYAN TYZ (CSB No. 234895)
ryan@tyzlaw.com
ERIN JONES (CSB No. 252947)
ejones@tyzlaw.com
DEBORAH HEDLEY (CSB No. 276826)
deborah@tyzlaw.com
STEPHANIE ALVAREZ SALGADO (CSB No. 334886)
stephanie@tyzlaw.com
TYZ LAW GROUP PC
4 Embarcadero Center, 14th Floor
San Francisco, CA 94111
Telephone: 415.868.6900

Attorneys for Defendant
Fandom, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

VISHAL SHAH, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FANDOM, INC.,

Defendant.

Case No: 3:24-cv-01062-RFL

DEFENDANT FANDOM, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS

Date: June 11, 2024
Time: 10:00 a.m.
Courtroom: 15, 18th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

NOTICE OF MOTION AND MOTION

TO THE COURT AND PLAINTIFFS AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on June 11, 2024, at 10:00 a.m. or as soon thereafter as counsel may be heard in Courtroom 15, 18th Floor of the above-entitled Court, located at 450 Golden Gate Avenue, San Francisco, CA 94102, Defendant, Fandom, Inc. will and hereby does move the Court for an order dismissing the Complaint of Plaintiff Vishal Shal pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. This Motion is based on the Notice of Motion and Motion, the Memorandum of Points and Authorities and the Request for Judicial Notice it contains, the Court's files in this action, the arguments of counsel, and any other matter that the Court may properly consider.

This Motion is based on the grounds that the Plaintiff's Complaint (the "Complaint") fails to state a claim upon which any relief may be granted and should thus be dismissed pursuant to Rule 12(b)(6).

Fandom respectfully requests that the Court (1) grant its request for judicial notice, and (2) issue an order dismissing the Complaint with prejudice under Federal Rule of Civil Procedure 12(b)(6) for failure to state any claim upon which relief may be granted.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff brings this putative class action against Fandom, alleging violation of California's criminal pen register statute. A pen register is a device or process that records a number dialed by a telephone. The California Legislature enacted California Penal Code 638.51 (the "California Pen Register Statute") for law enforcement to install and use a pen register to track to whom suspected criminals were talking. Plaintiff's Complaint attempts to turn this statute upside down.

Specifically, Plaintiff alleges that he visited Fandom's videogame-focused website Gamespot.com. Once he visited, two snippets of code developed by third-party vendors (the "Accused Code") were allegedly placed on his computer to track his IP address: a numerical identifier that enables a computer's browser to communicate with a website. According to Plaintiff, the Accused Code is an unlawful pen register under Section 638.51 because it captured his *source* IP address. But Plaintiff's attempt to state a claim under a statute that was enacted for a different purpose is readily apparent, and his claim fails as a matter of law for several reasons.

First, the Accused Code is not a pen register. At the most basic level, the Accused Code is not a pen register because it is not a device or process associated with telephonic dialing. Moreover, Plaintiff's allegations, attempting to contort this statute to apply to the use of the internet, does not comport with the intended mechanics of the Pen Register Statute. The text of the statute makes clear that it restricts surveillance of only the "routing, addressing, or signaling information" of a communication, this means information related to the telephone at the *receiving* end of a call. It does not extend, however, to information about the telephone *dialing* the call or, as alleged, the address of the computer making the request to a website.

Second, the Complaint does not allege transmission of any wire or electronic communication, a required element. Cal. Penal Code § 638.50. It only references the transmission of Plaintiff's source IP address without reference to any associated communication. Without identifying any communication, Plaintiff fails to plausibly allege that the Accused Code captures dialing or addressing information associated with an actual communication. To the

extent Plaintiff alleges that his IP address is contained within a communication, he still fails to state a claim because by definition, a pen register does not extend to cover "the contents of a communication." Cal. Penal Code § 638.50(b).

Third, the Complaint does not plausibly allege that Fandom "installed" or "used" the Accused Code. Instead, it alleges only that Fandom caused the Accused Code to be deployed by Plaintiff's browser but not that Fandom (rather than third parties) installed or used the Accused Code. And, even if Fandom had done so, installation or use of the Accused Code by Fandom is permitted under multiple exceptions to the statute.

Finally, Plaintiff fails to plausibly allege that the Accused Code *violated* his privacy interest because he does not have a reasonable expectation of privacy in his IP address. Even if his IP address was collected, that collection does not constitute the "injury" requirement to state a civil cause of action under the California Invasion of Privacy Act ("CIPA"), of which California's Pen Register statute 638.51 is part.

For any one of these reasons, the Court should reject Plaintiff's attempt to expand California's criminal pen register statute beyond its text and purpose. Otherwise, litigation covering the basic operation of accessing content on the Internet that the public has enjoyed for decades will continue to flood the Courts.[1] The Complaint should be dismissed.

II. RELEVANT FACTS

A. Gamespot.com

Fandom's website Gamespot.com (the "Website") is a popular, publicly-accessible video gaming website that provides news, reviews, previews, downloads, and other information about video games. Dkt. 1-1, ¶ 47. To access Gamespot.com (or any website on the Internet), a user must have and disclose an IP address associated with their computing device. *See id.*, ¶ 23. An IP address enables a "computer's browser [to] communicat[e] with a [website] server," and vice

[1] Plaintiff's counsel has filed a nearly-identical lawsuit against the Los Angeles Times, alleging the same claim under the California Pen Register Statute involving the same third-party code alleged in this case. *Taliah Mirmalek v. Los Angeles Times Communications,* Case No. 24CV063701, Superior Court of California, County of Alameda.

versa. *Id.* When a user visits the Website, the user's browser sends an "HTTP request" or "GET" request to Fandom's server. *Id.*, ¶ 20. When Fandom's server receives the HTTP or GET request, the server uses the device's IP address to send an HTTP response with instructions to the user's browser for how to display Gamespot.com, including "what images to load, what text should appear, or what music should play." *See id.*, ¶¶ 20, 21, 23.

Plaintiff alleges that Fandom's server caused the user's browser to also install two pieces of code (which Plaintiff calls "trackers"), from third parties GumGum and Audiencerate (collectively, the "Accused Code"), that recorded his IP address. *Id.*, ¶ 2.

B. The Accused Code

The only information allegedly collected by the Accused Code is a user's IP address which "enables" a user's browser to communicate with a website server. *Id.*, ¶ 23. The Accused Code allegedly instructs a user's browser to send that IP address to GumGum and Audiencerate in one of two ways: 1) "as standalone data" when a user visits the Website for the first time, or 2) in subsequent visits to the website, "through [a] cookie" allegedly installed by the Accused Code until the user clears the cookie from the user's cache. *Id.*, ¶¶ 29, 30, 41, 42, 73; *see also* fig. 4, 5 (showing GET request sent to GumGum and Audiencerate, not Fandom, allegedly containing IP address information). The Complaint does not allege that any user information, including the user's IP address, is communicated to Fandom's server as part of this process.

C. Plaintiff

Plaintiff claims to have visited the Gamespot website "multiple times" on his desktop browser. *Id.*, ¶ 71. Plaintiff alleges his IP address was sent to GumGum via the cookie installed by the GumGum code and to Audiencerate as standalone data (not via a cookie). *Id.*, ¶¶ 72-73.

III. LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a party may move to dismiss for "failure to state a claim upon which relief can be granted." Fed R. Civ. P. 12(b)(6). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is only plausible if the plaintiff alleges

enough facts to support a reasonable inference that the defendant is liable for the alleged misconduct. *Id.* A plaintiff must provide more than mere legal conclusions. *Twombly*, 550 U.S. at 555. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

When ruling on a Rule 12(b)(6) motion, the Court "accept[s] all factual allegations in the complaint as true." *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322 (2007). The Court, however, is "not bound to accept as true a legal conclusion couched as a factual allegation." *Twombly*, 550 U.S. at 555. Dismissal is appropriate "where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). That is the case here.

IV. ARGUMENT

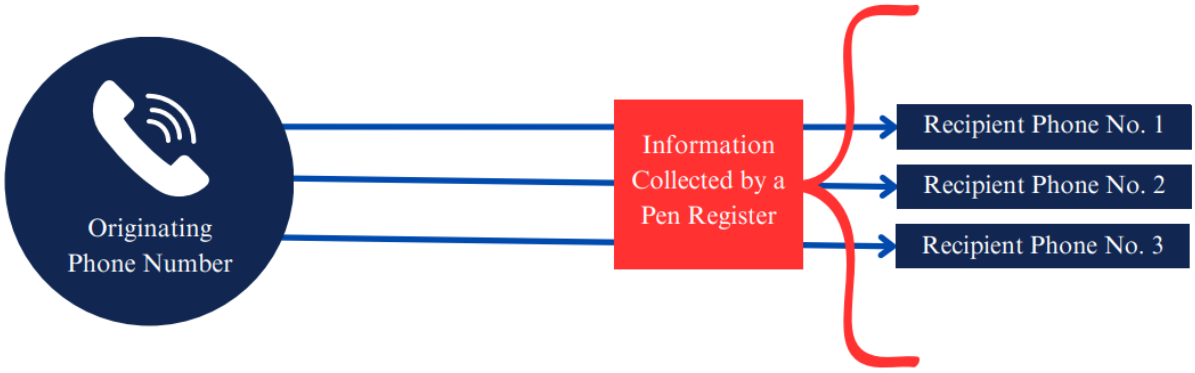
A. Plaintiff's Claim Fails because the Accused Code is Not a "Pen Register"

Plaintiff's Complaint does not allege facts that plausibly claim the existence of a pen register under the plain text of the statute and its legislative history. A "pen register" means "a device or process that records or decodes [the] dialing, routing, addressing, or signaling information" of an outgoing communication. Cal. Penal Code § 638.50(b). Here, the Accused Code is not a pen register because it is not a "device or process" that records or decodes "dialing, routing, addressing, or signaling information."

i. The Accused Code Does Not Record or Decode Any Dialing, Routing, Addressing, or Signaling Information for an Outbound Communication

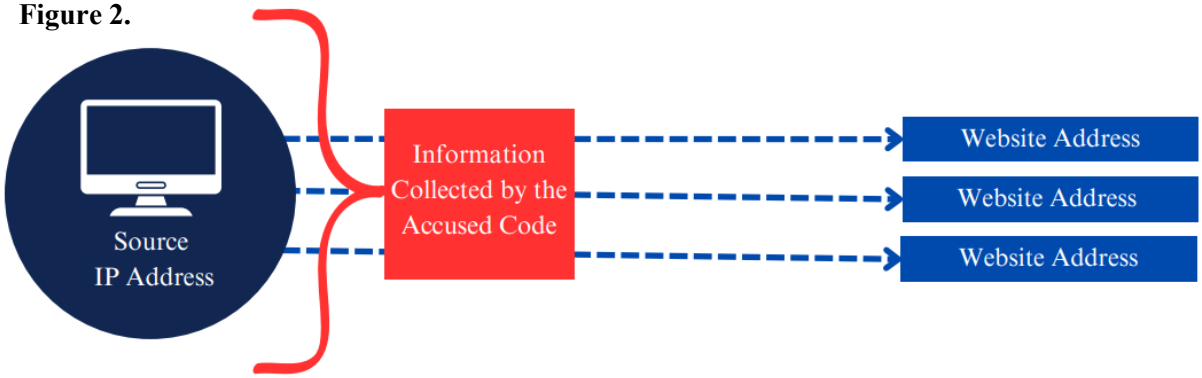
A pen register is a mechanical physical device installed on a landline telephone to measure *outgoing* electrical impulses, revealing the phone number being dialed—i.e., the recipient address of the communication. *See Smith v. Maryland,* 442 U.S. 735, 736 n. 1 (1979) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released."); *People v. Larkin*, 194 Cal. App. 3d 650, 653 n.2 (1987) ("A pen register is a mechanical device connected to a telephone number to monitor dialing activity. It registers the phone numbers dialed to make outgoing calls, including the dates and times the receiver is picked up and replaced."). To obtain this addressing

information, the pen register is appended to the telephone phone number ("originating phone number") that captures the phone number of *call recipients*. *See* Figure 1.



Here, Plaintiff alleges only that the Accused Code collected *his* computer's source IP address – nothing more. *See* Figure 2.

Figure 2.



Thus, what Plaintiff alleges to exist here is not a pen register under the plain reading of the statute because he does not allege that any *outgoing* addressing or routing information was recorded. Plaintiff does not allege, for example, that the Accused Code captured the IP addresses of the websites he visited. *See, e.g., United States v. Soybel*, 13 F.4th 584, 589 (7th Cir. 2021) (pen register installed by the government under the federal pen register statute "recorded connections *between* [Defendant's] private IP address and the IP addresses of those websites that internet users in the apartment had visited."). The Complaint only alleges the capture of Plaintiff's IP address but never explains how a user's source IP address, which at most reveals the general address of the device used to send some communication, is equivalent to the capture of routing or

addressing information for an *outbound* communication. *See* Dkt. 1-1 ¶ 23 ("Through an IP address, *the device's* state, city, and zip code can be determined.") (emphasis added).

Instead, the Complaint suggests that a device's source IP address may instead be information related to the source of an *incoming* communication – that is information Fandom's server receives from an incoming request to access the Website. But devices that log information relaying the source of an *incoming* communication are not pen registers. Rather, such devices are called "trap and trace" devices. Under California law, pen registers and trap trace devices are two distinct types of devices, defined by separate statutory provisions. *See* Cal. Penal Code § 638.50(b) (defining a "pen register"); Cal. Penal Code § 638.50(c) (defining a "trap and trace" device). Cal. Penal Code § 638.50(c) defines a "trap and trace" device as "a device or process that captures the *incoming* electronic or other impulses that identify the *originating number* or other dialing, routing, addressing, or signaling information reasonably likely to identify the *source* of a wire or electronic communication…[.]" (emphasis added). As the definition of a "trap and trace" device explicitly defines the device as one that captures "addressing" information relating to the "source" of an *incoming* communication—information like a user's source IP address allegedly captured by the Accused Code—it cannot be, as Plaintiff alleges, that a device that collects the same information is also a pen register, a device that by statute captures information relating to the opposite, receiving-end of a communication. *See California State Parks Found. v. Superior Ct.*, 150 Cal. App. 4th 826, 833 (2007) (courts "must select the construction that comports most closely with the apparent intent of the Legislature, with a view to promoting rather than defeating the general purpose of the statute, and avoid an interpretation that would lead to absurd consequences.") Here, Plaintiff only alleges the use of a pen register and does not allege the use of a trap and trace device—nor can he. Plaintiff cannot allege that the Accused Code is a trap and trace device because in order to "identify the source of [] wire or electronic communication[s]," a trap and trace device is installed at the *receiving* end of communications (here, Fandom's server), not the origin point of a communication (Plaintiff's browser), as alleged here. *Id.*

The statutory definition of a pen register is specific as to the type of data a pen register

must collect. Cal. Penal Code § 638.50(b). Having, at most, alleged that the Accused Code logged information relating to the *source* of an unidentified incoming communication, Plaintiff's claim under the California Pen Register Act fails because the Accused Code does not capture any dialing, routing, addressing, or signaling information of an outbound communication as required by Cal. Penal Code § 638.50(b).

ii. The Accused Code is Not a Device or Process

The legislative history of the California Pen Register Statute also makes clear that the purpose of the California Pen Register Statute was to protect individuals from the use of "device[s] or process[es]" that could be used for *telephone surveillance*. *See California Bill Analysis, A.B. 929 Assem*., 4/29/2015 ("This bill authorizes state and local law enforcement agencies to seek an emergency order to use pen registers and trap and trace devices in *telephone surveillance*") (emphases added); *see* 2015 California Assembly Bill No. 929, California 2015-2016 Regular Session (recognizing that pen registers are often "utilized by law enforcement to track which people in an investigation are communicating with one another and at what times" and noting that "[t]o date, California d[id] not have a state statute authorizing the use of pen registers or trap and trace devices."). Furthermore, other sections of California Penal Code § 638 confirm the term "pen register" is intended to have its traditional meaning. Section 638.52 which governs the application and authorization of use of a pen register by a law enforcement officer, provides that a pen register may not collect the physical location of the subscriber "except to the extent that the location may be determined *from the telephone number*." Cal. Penal Code § 638.52 (emphasis added). Further, 638.52 clarifies that any court order authorizing law enforcement to use a pen register must include the identity of the person associated with the "*the telephone line* to which the pen register…is to be attached." *Id*. (emphasis added).

Nothing in the California Penal Code extends a pen register to software on a computer. Indeed, the "device or process" required under Section 638.50 must be tied to "telephonic functionality," and a plaintiff fails to plead the use of a "device" under the Section 638.50, where the complaint does not include "any actual specific reference to a mobile phone or other potential form of communication device potentially qualifying as a cellular device." *Jose Licea vs. Hickory*

Farms LLC, Case No. 23STCV26148, Superior Court of California, Central District, Minute Order, dated March 13, 2024 (Attached as Exhibit 2). Here, the Complaint merely alleges that the Accused Code collected the IP address of a "*desktop browser*" Plaintiff used to visit the Website. Dkt. 1-1., ¶¶ 71, 89. Accordingly, Plaintiff's claims fail because the Accused Code is not a device or process associated with telephonic surveillance.

Nonetheless, the Complaint alleges, as a conclusion, that the Accused Code "is at least a 'process'" under California Penal Code § 638 because it is "software that identifies consumers, gathers data, and correlates that data," parroting language from an out-of-district court, *Greenley v. Kochava*, Inc., No. 22-CV-01327-BAS-AHG, 2023 WL 4833466, at *15 (S.D. Cal. July 27, 2023). In *Greenley*, however, the court did not hold that *any* software that identifies consumers, gathers data, and correlates that data is a pen register. Instead, the court limited its holding to finding that "surreptitiously embedded software installed in a *telephone*" that "identifies consumers, gathers data, and correlates that data through unique fingerprinting" pinning them to a precise geolocation could be a pen register. *Id.* (emphasis added). The facts of that case are vastly different than here.

Here, Plaintiff fails to allege that the Accused Code was used in conjunction with telephonic dialing or that it collected any type of information that would enable Fandom to generate such a "unique fingerprint" for a website user. *See id.* at 15. There is no allegation that the Accused Code captures cell phone geolocation data of the type alleged in *Greenley*, which is fundamentally different than the IP addresses of a computer. Indeed, an IP address is necessary to access any website, and it simply cannot be that a website violates California's pen register statute anytime a website's server logs the IP address of a device seeking access to the website. Courts given the opportunity to consider this issue under the federal pen register statute have recognized the risks of holding otherwise, finding that the federal "Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, **then the Internet could not function** because standard computer operations require recording IP addresses so parties can communicate with one another over the Internet." *Capitol Recs. Inc. v. Thomas-Rasset*, No. CIV 06-

1497(MJD/RLE), 2009 WL 1664468, at *3 (D. Minn. June 11, 2009) (emphasis added).

As the Complaint only alleges the existence of code that collects a user's IP address, Plaintiff has failed to plead the existence of a pen register, i.e. a "device or process" within the meaning of the CIPA and the Complaint must be dismissed.

B. Plaintiff Fails to Allege the Transmission of a Communication between Plaintiff and Fandom

Plaintiff's Complaint further fails because it does not identify that a wire or electronic communication was transmitted. The definition of "pen register" under the CIPA differentiates two types of information relating to the transmission of a communication: the "dialing, routing, addressing, or signaling information" of a communication and 2) "the contents of a communication." Cal. Penal Code § 638.50(b). Because the definition of pen register centers on the type of information that may or not be gathered from the fact of a communication, to plead a claim under the CIPA, a Plaintiff must first allege the transmission of a communication whose dialing information was registered. But the Complaint fails to allege this essential element.

Nowhere in the Complaint does Plaintiff identify any "communication" whose "dialing, routing, addressing, or signaling information" was allegedly collected by the Accused Code as required by Cal. Penal Code § 638.50(b). Plaintiff states only, as a conclusion, without supporting facts, that the Accused Code is installed and then "instructs the user's browser to send" GumGum and Audiencerate "the user's IP address." Dkt. 1-1, ¶¶ 28, 40. But the Complaint neither claims nor explains how the Accused Code supposedly obtained the IP address associated with a specific "communication." Indeed, the word "communication" only appears in statements quoting or summarizing the language of the CIPA and in one barebones allegation *disclaiming* that this litigation involves communication: "The [Accused Code] do[es] not collect the content of Plaintiff's and the Class's electronic communications with the Website." *Id.*, ¶ 91. This is true – the Complaint does not allege that the Accused Code collected the content of any communication, but, detrimentally to Plaintiff's claim, the Complaint also fails to identify the transmission of *any* communication between Plaintiff to the Website. Without communication there is no addressing information for any alleged pen register to "decode or record" as required by statute. Cal. Penal

Code § 638.50(b).

Further by failing to identify any communication, the Court cannot determine whether the IP address is part of the contents of a communication. To the extent Plaintiff is alleging that his IP address is part of the substance of the communication with Fandom, his IP address would then fall outside the scope of the California Pen Register Statute. *See* Cal. Penal Code § 638.50(b) (defining "pen register" as a device or process that does not decode or record "the contents of a communication."); *see also Capitol Recs. Inc.*, 2009 WL 1664468, at *3 (federal pen register act "ha[d] no application…because the IP address recorded by MediaSentry was part of the content of the communication.").

The closest Plaintiff gets to pleading a communication was made, is when Plaintiff suggests that the IP address is sent as the *content* of a communication—not between Plaintiff and Fandom—but between Plaintiff's browser and third-party GumGum's and Audiencerate's servers. *See e.g., Dkt*. 1-1, ¶ 29, (Accused Code "instructs the user's browser to send the user's IP address through the cookie"), ¶ 73 ("IP address is transmitted within the cookie"). In his Complaint, Plaintiff explains that his IP address was sent both "as standalone data" and "within [a] cookie" to GumGum and Audiencerate.[2] *Id*., ¶ 73. This description, however, only highlights that Plaintiff's IP address is "merely passively conveyed through third party equipment" as "standalone" content or content "within [a] cookie" to GumGum's and Audiencerate's servers, rather than serving as routing or addressing information for an outbound communication. *Compare with United States v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008) (noting that "IP addresses *are not merely passively conveyed* through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers") (emphasis added).

Therefore, Plaintiff seems to, in effect, be arguing that the IP address might instead be more closely related to the *content* of a communication between Plaintiff's browser and GumGum's and Audiencerate's servers, than its addressing information. But a device that collects the contents of a communication cannot, by definition, be a pen register. Cal. Penal Code

[2] Plaintiff does not allege that the Accused Code sent Plaintiff's IP address to Fandom's server.

§ 638.50(b) (defining "pen register" as a device or process that does not decode or record "the contents of a communication."). Further, case law under the expansive federal pen register statute similarly suggests that where a device conveys an IP address as the content of a communication, such a device is not a pen register. *See e.g., In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) ("In essence, addresses, phone numbers, and URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function. If an address, phone number, or URL is instead part of the substantive information conveyed to the recipient, then by definition it is 'content.'"); *Malibu Media, LLC v. Pontello*, No. 13-12197, 2013 WL 12180709, at *4 (E.D. Mich. Nov. 19, 2013) ("In the instant case, the IP address received by IPP was part of the content of the communication, so the Pen Register Act has no application. By participating in the BitTorrent swarm Pontello consensually engaged in the transaction with IPP, and communicated his IP address as part of the packet his computer sent to IPP."); *Capitol Recs. Inc,* No. 2009 WL 1664468, at *3 ("The Pen Register Act has no application here because the IP address recorded by MediaSentry was part of the content of the communication.").

Thus, to the extent Plaintiff's Complaint is read to mean the Accused Code captures the contents of a communication between Plaintiff's browser and GumGum's and Audiencerate's servers (i.e., Plaintiff's IP address), the Accused Code would fall outside the definition of a pen register, a device which by statutory definition cannot collect the contents of a communication. Plaintiff's claim under the California Pen Register Statute thus again fails because the Complaint fails to identify a communication for which the Accused Code could even decode or record dialing, routing, addressing, or signaling information.

C. Plaintiff Does Not Plausibly Allege that Fandom "Installed" or "Used" the Accused Code, and Even So, Fandom Is Permitted by the Statute to Do So

Plaintiff does not plausibly allege that Fandom "install[ed] or use[d]" the alleged pen register, as 638.51(a) requires. Instead, the Complaint alleges that third-parties, GumGum and Audiencerate, develop, install, and use the Accused Code. *See* Dkt. 1-1, ¶¶ 25, 36.

Although Plaintiff alleges, as a conclusion, that Fandom installed the Accused Code on

his browser, Plaintiff does not allege any facts to plausibly support that conclusory allegation. *See Iqbal*, 556 U.S. at 678 (2009) ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."). Plaintiff instead uses many words to skirt this issue, alleging that Fandom incorporated, programmed, and "caused to be installed" the Accused Code while failing to explain plausibly how Fandom installed the Accused Code on his browser. *Id.*, ¶¶ 51-52. Indeed, as recognized by the Complaint, the Accused Code is software developed and used by third parties GumGum and Audiencerate, and not by Fandom. *Id.*, ¶¶ 25, 36; *compare with Greenley,* 2023 WL 4833466, at *1 (Plaintiff sued the developer of the software alleged to be a pen register, not the app creators that used the developer's code in their apps with the code where defendant-developer "coded its [software] for data collection and embedded it in third-party apps…secretly collected app users' data; and then Defendant packaged that data and sold it to clients for advertising purposes."). Plaintiff thus fails to plead sufficient facts to nudge his Complaint from Fandom *possibly* installing the Accused Code, to Fandom *plausibly* installing the Accused Code, and consequently fails to state this element. *See e.g., Esparza v. Lenox Corp.*, No. C 22-09004 WHA, 2023 WL 2541352, at *3 (N.D. Cal. Mar. 16, 2023) (finding that "[w]ithout further elaboration, plaintiff's allegations that someone eavesdropped and intercepted chat messages [were] merely conclusory recitations of the CIPA wiretapping statute, and not entitled to the presumption of truth;" "Plaintiff's claim of a CIPA violation [wa]s therefore insufficient to withstand dismissal.").

The Complaint also fails to allege that Fandom used the alleged Accused Code. Indeed, the crux of Plaintiff's Complaint is not that Fandom may have used the Accused Code to discover his IP address. The Complaint instead stresses that the data allegedly collected by the code (Plaintiff's IP address) was sent directly to and was used by GumGum and Audiencerate. Dkt. 1-1,¶62 ("GumGum collects IP addresses"), ¶ 28. ("The GumGum Tracker, in turn, instructs the user's browser to send GumGum the user's IP address."); ¶ 69 ("Audiencerate collects IP addresses"); ¶ 40 ("The Audiencerate Tracker, in turn, instructs the user's browser to send the user's IP address to Audiencerate.).

Even if Fandom installed or used the Accused Code, which it did not, and even if the

Accused Code were a pen register, which it is not, then Fandom's actions were permissible under the statute as the Pen Register statute allows a "provider of electronic …communication service" to "use a pen register or a trap and trace device 1) [t]o operate, maintain, and test a wire or electronic communication service" or 2) "where consent of the user of that service has been obtained." Cal. Penal Code § 638.51(b).

i. Fandom is Allowed to Collect IP Addresses to Operate Its Website

Here, Fandom is a provider of electronic communication service. "Electronic communication" means "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system." Cal. Penal Code § 629.51. Fandom allows for electronic communication via its public website Gamespot.com because it allows data to be delivered to a website user. *See* Dkt. 1-1, ¶47. But, for Fandom's website to operate and load, a user must first have an IP address because IP address enables Fandom's server to load the data the user is seeking, for the user. *See id*., ¶ 23. Under such circumstances, the alleged collection of IP address is permitted by statute. *See, e.g., Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *11 (C.D. Cal. May 29, 2007) (holding the "collection of incoming IP addresses by defendants [wa]s exempt" pursuant to an exception to the federal pen register statute allowing "providers of electronic communication services" to use a pen register or trap and trace devices to operate and maintenance of such service because "defendants already and necessarily capture[d] such data …to operate the website.").

ii. Plaintiff Consented to Fandom Knowing His IP Address

Furthermore, Plaintiff *necessarily* consented to the collection of his IP address by Fandom, and thus Fandom is exempted from liability for any alleged record of his IP address with a pen register. IP addresses "are voluntarily turned over in order to direct . . . third party[] server[s]" and so no reasonable expectation of privacy attaches to them. *Forrester*, 512 F.3d at 503. Here, Plaintiff voluntarily presented his IP address to the Website's server "multiple times" in order to access the Website and Plaintiff cannot now plausibly claim that he did not consent to Fandom's alleged use of a device or process to decode or record his IP address. *See* Dkt. 1-1, ¶

71. Moreover, Fandom's Website's Privacy Policy[3] specifically informs users of the type of technologies employed on the Website, establishing explicit consent, as well as providing California users an opportunity to prohibit data sharing, direct Fandom to delete their information and take other steps required by California law. *See* https://www.fandom.com/privacy-policy-pp1 (Exhibit 1). The Privacy Policy notifies visitors that Fandom may collect their IP address during a user's visit to the Website to provide advertising relevant to its users. *See id.* ("In order to provide advertisements relevant to you, your IP address may be used, as well as your operating system and device type.").

D. The Alleged Use of the Accused Code Did Not Cause a Privacy Injury

The CIPA was enacted "to protect the right of privacy of the people of this state." Cal. Penal Code § 630. And individuals "injured by a violation of" the CIPA can bring a private right of action under §637.2. As explained by the Supreme Court of California, in enacting the CIPA, "the Legislature declared in broad terms its intent 'to protect the right of privacy of the people of this state' from what it perceived as 'a serious threat to the free exercise of personal liberties [that] cannot be tolerated in a free and civilized society. This philosophy appears to lie at the heart of virtually all the decisions construing the Invasion of Privacy Act." *Smith v. LoanMe*, Inc., 11 Cal. 5th 183, 199 (2021) (citing to *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985)).

Plaintiff's claim fails because he has not and cannot plausibly allege that he has suffered a privacy injury. Plaintiff alleges that the "[t]he collection of" his "personally identifying, non-anonymized information through [Fandom]'s installation and use" of the Accused Code

[3] Plaintiff's Complaint centers on what occurred when Plaintiff visited the Website, as the Website's Privacy Policy is linked-on the Website, the terms are incorporated by reference into the Complaint. The Court may also take judicial notice of the Privacy Policy because it governs Plaintiff's interaction with the Website, which forms the basis of Plaintiff's Complaint. *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1065 n.24 (N.D. Cal. 2014) (taking notice of agreement governing transaction at heart of complaint). In addition, the Website's Privacy Policy was publicly published online, and its authenticity cannot reasonably be questioned. *In re Google, Inc. Priv. Pol'y Litig.,* No. C 12-01382 PSG, 2012 WL 6738343, at *4 (N.D. Cal. Dec. 28, 2012) (judicially noticing a website's privacy policy on the grounds that it was published online and thus "a matter of public record" and separately because "Plaintiffs' complaint necessarily relied upon" it). Fandom requests that the Court take judicial notice of Fandom's Privacy Policy attached as Exhibit 1.

"constitutes an invasion of privacy." Dkt. 1-1, ¶ 56. However, the only information the Accused Code allegedly collected was Plaintiff's source IP address. Plaintiff identifies no other type of information collected, let alone any "personally identifying" information allegedly collected. The collection of IP addresses alone does not constitute a privacy injury.

Indeed, the Ninth Circuit has, on multiple occasions, concluded that Internet users do not have reasonable expectations of privacy in their own IP addresses or the IP addresses of the websites they visit. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) ("Internet users have no expectation of privacy in the ... IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing information."); *United States v. Heckenkamp*, 482 F.3d 1142, 1148 (9th Cir. 2007) (holding that a defendant had "no reasonable expectation of privacy" in "network logs" that contained his computer's IP address); *United States v. Rosenow*, 50 F.4th 715, 738 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 786 (2023) (finding that Defendant "did not have a legitimate expectation of privacy in the limited digital data sought" by a government subpoena, where the subpoena called for the production of Defendant's IP addresses).

The Ninth Circuit has made it clear that internet users, like Plaintiff, have no expectation of privacy in IP addresses because they should know that this information is provided to and used by Internet service providers and third-party servers for the purpose of directing the routing of electronic information. *See Forrester*, 512 F.3d at 510. Consequently, Plaintiff's claim fails because even if the Accused Code works as claimed in the Complaint (it does not), Plaintiff's privacy rights are not infringed by the alleged use of the Accused Code. Plaintiff cannot state a claim under the CIPA for the fundamental reason that he never had a right to privacy over the only information identified in this case, his source IP address.

V. CONCLUSION

For all these reasons, the Court should grant the Motion and dismiss Plaintiff's Complaint without leave to amend. Plaintiff's attempt to characterize as a pen register a piece of code that captures a user's IP address (and nothing more) stretches the language and meaning of the CIPA. Plaintiff's misguided reasoning would turn any single record of an online user's IP address made

by a website server, an act much like writing down or saving a phone number of a person that shared their number in hopes of receiving a call, into an unlawful pen register.

Respectfully submitted,
TYZ LAW GROUP PC

Dated: April 8, 2024

/s/ Stephanie Alvarez Salgado
Stephanie Alvarez Salgado

Attorneys for Defendant
FANDOM, INC.